UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,501	12/12/2003	Sudarshan Palliyil	JP920030154US1	1612

39903 7590 03/16/2007

ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	PAPER NUMBER
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/734,501	PALLIYIL ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/12/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/12/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-38 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-8, and 13-15, 21, 24, and 29 are rejected under 35 U.S.C. 102(b) as being anticipated by Nachenberg (US 6,021,510).

Regarding claim 1:

Nachenberg discloses a method for identifying data processing systems within a network having a vulnerability comprising: computing a set of hash values representing a set of resources for which an operation has been performed (column 4 lines 5-8); storing the set of hash values (column 4 lines 5-8); in response to a requirement for performance of the operation, computing a new set of hash values representing the set of resources (column 4 lines 40-47); comparing the new hash values with the stored hash values for the set of resources to identify matches between new hash values and stored hash values (column 4 lines 48-63); determining that performance of the operation is not currently required for resources for which a match is identified between the respective new hash value and a stored hash value (column 4 lines 48-53); and performing the operation for resources for which no match is identified between the new hash value and any stored hash value (column 4 lines 54-63).

Regarding claim 2:

Nachenberg discloses the method of claim 1, wherein the operation comprises scanning the resources to identify computer viruses (column 4 lines 54-63).

Regarding claim 3:

Nachenberg discloses the method of claim 1, wherein the operation comprises making a backup copy of the resources (column 4 lines 58-63, the file is moved to disk, creating an effective backup; additionally, Norton AntiVirus (column 3 lines 14-15, its features are incorporated by reference) has the ability to create a backup on the quarantine server, see *Norton AntiVirus Enterprise Solution 4.0*).

Regarding claim 4:

Nachenberg discloses the method of claim 1, for controlling performance of virus scanning and backup copy operations in relation to a set of resources within a data processing network, the method comprising: using said identification of a match between a respective new hash value and a stored hash value for a resource, resulting from a single comparison of new and stored hash values, to determine that neither virus scanning nor backup copy operations are currently required for the resource (column 4 lines 48-53).

Regarding claim 5:

Nachenberg discloses the method of claim 1, wherein the step of computing a new set of hash values comprises reading the set of resources from a first storage medium into a second storage medium which provides faster access than the first storage medium and computing the set of hash values (column 4 lines 29-31), and

wherein the method further comprises: comparing each of the set of resources with a maximum size limit to identify resources within said set which are smaller than said size limit (it is inherent that the data does not exceed the storage threshold of said second storage, this is a common feature of memory management), and retaining said smaller resources within said second storage medium to enable further operations (it is inherent to hold only the amount that is available in said second storage, Nachenburg teaches the use of sectors (column 3 line 66 to column 4 line 10), which are fractions of the original file).

Regarding claim 6:

Nachenberg discloses the method of claim 1, wherein the operation comprises transferring a resource across a low bandwidth communication channel (Norton AntiVirus (column 3 lines 14-15) has the ability to create a backup on the centralized, quarantine server (inherently requires a low-bandwidth communication channel to send the information from host/server to server), see *Norton AntiVirus Enterprise Solution 4.0*).

Regarding claim 7:

Nachenberg discloses the method of claim 1, wherein the steps of computing hash values comprise: applying a secure hash function to a bit pattern representing a resource, for each of a set of resources (column 1 line 60 to column 2 line 9). It is inherent that the hash would have been a secure hash as secure hashes were common at the time of invention as is shown in Bruce Schneier's *Applied Cryptography, 2d ed.* (Chapter 18 - *One-Way Hash Functions*).

Regarding claim 8:

Nachenberg discloses the method of claim 7, wherein the set of resources for which hash values are computed for a data processing system comprises the set of all files of executable file types on the system. Nachenburg discloses a method for examining files associated with a digital computer (column 1 lines 60-63). It is an inherent trait of anti-virus software to scan all executable file types on the system.

Regarding claims 13 and 14:

Nachenberg discloses the method of claim 1, wherein at least one resource of the set of resources comprises a group of files (column 3 lines 14-15 discloses the use of Norton AntiVirus (NAV) which contains the capability of scanning compressed files (see *Norton AntiVirus Enterprise Solution 4.0*)) and the step of computing a set of hash values comprises computing a single hash value for the group of files (it is inherent that the invention disclosed by Nachenburg would use the method for scanning a file applied to scan the compressed file).

Regarding claims 15 and 24:

Nachenberg discloses a method for controlling scanning for computer viruses within a data processing network, comprising the steps of: computing a set of hash values representing a set of resources which have been determined to be virus-free (column 3 line 55 to column 4 line 8); storing the set of hash values (column 4 lines 5-8); in response to a requirement for a virus check, computing a new set of hash values representing the set of resources (column 4 lines 40-47); comparing the new hash values with the stored hash values for the set of resources to identify matches between

new hash values and stored hash values (column 4 lines 48-63); determining that no virus scan is currently required for resources for which a match is identified between the new hash value and a stored hash value (column 4 lines 48-53); and performing a virus scan for each resource for which no match is identified between the new hash value and any stored hash value (column 4 lines 54-63).

Regarding claims 21 and 29:

Nacheberg discloses the method of claim 15 and 24, wherein the step of determining that no virus scan is currently required for resources for which a match is identified comprises the following steps: identifying a subset of resources within said set of resources for which a match is identified between the new hash value and a stored hash value (column 4 lines 48-53); determining whether each resource within said subset has been classified virus-free by each of a plurality of virus scans of the resource at scan times which differ by more than a threshold; and determining that no virus scan is currently required for each resource for which a positive determination is made that the resource has been classified virus-free by each of a plurality of virus scans at scan times which differ by more than the threshold (it is inherent that virus scanners have a periodic scanning feature and that files are considered virus free if no virus was detected in any of the periodic scans).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims 9-12, 16-19 and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg as applied to claims 1, 15, and 24 above, and further in view of Feigen et al. (US 2002/0138554).

Regarding claims 9-12, 16-19, 25-27:

Nachenberg discloses the method of claim 1, but it does not disclose storing hash values and comparing the hash values at a first data processing system. Feigen et al. discloses the method wherein the host hashes a block of code (figure 2, 202),

transmits parameters to client (204), the remote device hashes and determines hash value (206 and 208), and sends the hash to host for comparison by host (210 and 212). In paragraph 0016, Feigen et al. discloses that if the two hash values are identical, the host confirms that the code at the resident has not been tampered with. Additionally, Feigen et al. discloses that if the two hashes are not identical, then the host may take additional action. It would have been obvious to incorporate a virus scan or backup into the additional action as disclosed by Nachenberg in order to check if a virus is present.

4. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg and Feigen et al. as applied to claim 16 above, and further in view of Albrecht (US 2001/0005889). Nachenberg and Feigen et al. disclose the method of claim 16, but they do not disclose receiving a copy of the resource, performing a virus scan of said resource, and reporting the result of the virus scan. Albrecht discloses receiving the copy of the resource at the first data processing system (figure 3, agent returns file portions, paragraph 0048), performing a virus scan of said resource at the scanning engine (paragraph 0048), and reporting the result of the virus scan to the agent (paragraph 0048). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method disclosed by Nachenberg and Feigen et al. with the centralized scanning engine of Albrecht in order to reduce maintenance overheads for the anti-virus applications (paragraph 003).

5. Claims 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg as applied to claim 15 above, and further in view of Nachenberg.

Nachenberg discloses the method of claim 15, further comprising: comparing the new hash value computed for a first resource with hash values computed for other resources of said set of resources, to identify matching hash values indicating replicated resources; in response to determining that a virus scan is currently required for the first resource, performing a virus scan of the first resource; and recording a result of the virus scan of the first resource as a virus scan result for any replica resources (it is inherent that a database maintains the data to be consistent (existing with the same values for like files)). The method of claim 22, wherein the set of resources is distributed across a plurality of data processing systems within a network, the method further comprising: forwarding an indication of the result of the virus scan to the data processing systems storing the first resource and any replica of the first resource within the network. It would be obvious to modify the method of Nachenberg to notify the other systems in the network in order to maintain database consistency.

6. Claims 37 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg. Nachenberg teaches all of the limitations of claim 37 in claim 1, 5,or 24, but it does not teach the use of decoys. It is well known in the art to use a method of decoy systems also known as honeypots. It would have been obvious to one of ordinary skill in the art to alter the method claim of 1, 15, or 24 in order to log attacker's methods and motives of intruding into a system..

Regarding claims 30-36:

7. Claims 30-36 teach the system or software on a storage medium associated with

the method claims disclosed in the rejection of claims 1-29. Claims 30-36 are rejected under the same logic.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses distributed systems, remote integrity checking, and antivirus systems and methods.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Taghi T. Arani
Primary Examiner
Taghi T. Arani
3/13/04